

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) Publication number:

0 409 397 A2

(12)

EUROPEAN PATENT APPLICATION

(21) Application number: 90306141.4

(51) Int. Cl.⁵: G06F 1/00

(22) Date of filing: 06.06.90

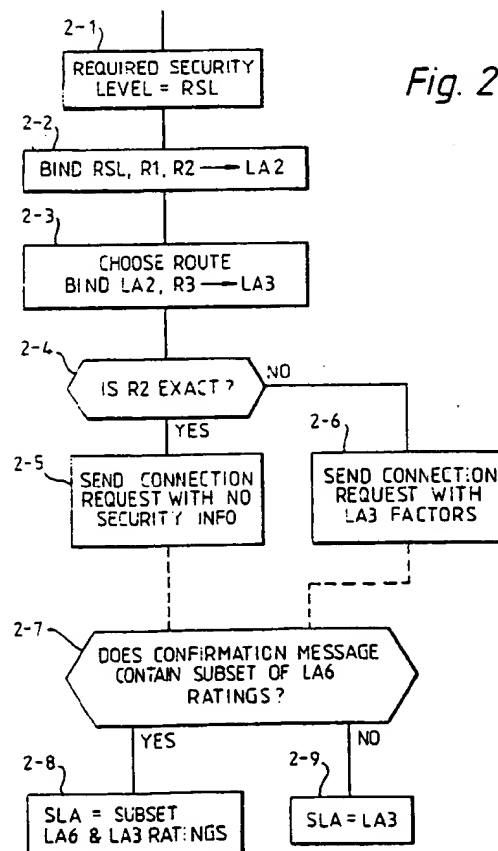
(30) Priority: 20.07.89 GB 8916586

(43) Date of publication of application:
23.01.91 Bulletin 91/04(84) Designated Contracting States:
BE DE FR GB IT(71) Applicant: **INTERNATIONAL COMPUTERS
LIMITED**
ICL House

Putney, London, SW15 1SW(GB)

(72) Inventor: **McVitie, David Glen**
Brunswick House, Brunswick Street
Congleton, Cheshire CW12 1QF(GB)(74) Representative: **Guyatt, Derek Charles et al**
STC Patents West Road
Harlow Essex CM20 2SH(GB)(54) **Distributed data processing system.**

(57) A security mechanism is described for a distributed data processing system. Each server in the system maintains a set of security ratings giving its view of the security levels within the system. When a first server wishes to initiate a connection with a second server, the two servers exchange security information, by means of messages, so as to establish an overall security level for the connection, based on a combination of the security information maintained by both servers. However, if the first server decides that the second server cannot be trusted to discuss security, messages are exchanged containing no security information, and each server establishes its own security level for the connection, based on its own locally held security information.

**EP 0 409 397 A2**

DISTRIBUTED DATA PROCESSING SYSTEM

Background to the invention

This invention relates to distributed data processing systems. More specifically, the invention is concerned with a data processing system comprising a number of servers connected together by one or more interconnection routes. By a "server" is meant a unit that provides some service to the system; for example, a computer unit which provides a data processing service or an electronic mail service. The interconnection routes may, for example, comprise a local area network (LAN) or a telephone link.

The invention is particularly concerned with federated computer systems. A federated system is a distributed data processing system in which there is no central controller or data store. Each server is capable of operating autonomously, and there is no master unit for directing the operation of the system.

In such a system, servers can exchange information by setting up connections between them, by way of the interconnection routes. Each such connection between two servers is asymmetric, in that the server at one end starts the connection process. This server is referred to herein as the initiator, while the server at the other end is referred to as the responder.

In a federated system, one important consideration is that of security, i.e. of ensuring that only those with permission to access servers do so. In particular, when a connection is requested, some check has to be made concerning the validity of that connection. Thus, a check must be made as to whether the responder is sufficiently secure to meet the needs of the initiator, whether there is a suitable route between the two servers that will preserve the security of their conversations, and whether the responder is prepared to be used by the initiator.

This problem of providing security is made more difficult by the completely distributed nature of the system, and by the fact that there is no single central authority to control the security of the system.

The object of the present invention is to provide a novel way of overcoming the problem of providing security in a federated system.

Summary of the invention

According to the invention there is provided a distributed data processing system comprising a plurality of servers wherein each server separately

maintains security information relating to security levels in the system, and wherein, in operation, when a first server initiates a connection with a second server, these two servers exchange security information to establish an overall security level for the connection based on a combination of the security information maintained by both servers.

Brief description of the drawings

Figure 1 is a block diagram of a distributed data processing system.

Figure 2 is a flow chart showing the operations performed by an initiator in setting up a proposed connection.

Figure 3 is a flow chart showing the operations performed by a responder in setting up a proposed connection.

Description of an embodiment of the invention

One distributed data processing system in accordance with the invention will now be described by way of example with reference to the accompanying drawings.

Overall view of the system

Referring to Figure 1, the distributed data processing system comprises a plurality of servers 10, 11, 12 interconnected by routes 13, 14.

For example, the servers may comprise free-standing computers, each of which is capable of independent operation, as well as contributing a service to the system as a whole. The interconnection routes may comprise local area networks (LANs) or telephone links.

The system is organised as a federated system; that is, there is no central controller or store for controlling the operation of the system as a whole. Instead, the responsibility for system control is shared among the individual servers.

Security in the system is described by means of security levels which can be assigned to servers and to routes between servers. Because of the federated nature of the system, there is no single repository of information about security levels in the system. Instead, each server maintains its own local view of the security levels in the system. This consists of a table containing a security rating for each server in the system, and for each interconnection route. It is important to note that the local views held in different servers may not be the

same; for example, different servers may give a particular route different security ratings.

Security ratings

Each security rating comprises a set of security factors, where each factor in turn comprises a set of values. For example, a security rating for a particular server might be:

(COLOUR = (RED, BLUE, YELLOW), DAY = (MONDAY))

This consists of two factors COLOUR and DAY, where the factor COLOUR consists of three values RED, BLUE and YELLOW, while the factor DAY consists of just a single value MONDAY.

In this example, this security rating indicates that the server is entitled to receive electronic documents with status codes RED, BLUE or YELLOW only, and only on Monday.

A security factor that contains just a single value (such as the factor DAY above) is referred to herein as an exact factor, since it indicates that a particular condition must be matched exactly. Conversely, a factor that consists of more than one value (such as the factor COLOUR in the above example) is referred to herein as an inexact factor, since it indicates that there is a degree of choice about this factor. Similarly, a security rating that contains only exact factors is referred to as an exact rating, while a rating that contains one or more inexact factors is referred to as an inexact rating.

Default ratings

The following rules are specified to cover default conditions, where some or all of the information in a security rating is omitted.

- (i) If a security rating is omitted completely, it is assumed that this is equivalent to a rating comprising all possible factors with all possible values present.
- (ii) If a factor is omitted from a security rating, it is assumed that this is equivalent to the factor being present with all possible values.
- (iii) An empty factor (i.e. one with no values) is not allowed. However, it is possible to give a factor a special NULL value.

Binding security ratings

In operation of the system, different security ratings may be combined by a process referred to as binding. This consists of forming the logical intersection of the ratings, to produce a resultant

rating consisting of values common to all these ratings. Where a particular factor is not present in one or more of the ratings, the above default rules apply.

For example consider the two ratings:

(DAY = (SAT, SUN, MON), COLOUR = (RED, BLUE))

(DAY = (MON, TUE))

The result of binding these two ratings will be:

(DAY = (MON), COLOUR = (RED, BLUE))

It should be noted that, in this example, the factor COLOUR is not present in the second of the ratings, and it is therefore assumed as a default condition, that this factor is present with all possible values.

Initiating a connection

Before any two servers can exchange information, a logical link, referred to herein as a connection, must first be set up between them. The server that initiates the connection is referred to as the initiator and the other server is referred to as the responder.

As mentioned above, the security level of a server or route is not known in an absolute manner by a single authority. Rather, the security level ascribed to a particular connection depends on an interaction between the initiator and responder, taking account of the locally held security ratings in each of them.

The following list indicates the various security ratings that may influence the security level of a particular proposed connection.

R1: the initiator's rating of itself.

R2: the initiator's rating of the responder.

R3: the initiator's rating of the route or routes available to connect to the responder.

R4: the responder's rating of itself.

R5: the responder's rating of the initiator.

R6: the responder's rating of the route chosen by the initiator.

Initiator

Referring now to Figure 2, this shows the operation of the initiator in setting up a connection.

(2-1) The initiator specifies a required security level (RSL) for the connection.

(2-2) The initiator then binds the level RSL with the ratings R1 and R2 to produce a resultant security rating LA2. If LA2 is empty (i.e. there are non intersecting ratings in RSL, R1 and R2) then the attempted connection has failed, since it is not possible to satisfy the security requirements of the initiator.

(2-3) The initiator now selects a route to the responder, and binds the security rating R3 of this chosen route with LA2 to produce a resultant security rating LA3. If it is not possible to find a route for which LA3 has non-empty ratings, the attempted connection fails.

(2-4) The next action taken depends on whether the rating R2 (i.e. the initiator's view of the security rating of the responder) is exact or inexact.

(2-5) If the rating R2 is exact (i.e. contains only exact factors as defined above), this means that the initiator does not trust the responder to discuss security. That is, the responder cannot be trusted to receive security information or to make decisions about security levels, and the initiator must take all responsibility for the security of the connection.

In this case, therefore, the initiator sends a connection request message to the responder, containing no security information.

(2-6) If, on the other hand, R2 is inexact (i.e. contains at least one inexact factor), this means that the initiator considers that the responder is capable of discussing security levels. The initiator therefore transmits a connection request message to the responder, containing all the factors of LA3 that correspond to inexact factors of R2. These factors represent the initiator's view of what the responder has to know about the required security level. Factors in LA3 which correspond to exact factors in R2 are not transmitted, since the initiator believes that the responder is not capable of discussing these factors.

The net result is that the initiator sends only security information on which it believes the responder can be trusted to behave correctly. If it does not trust the responder at all, it sends no security information to it.

Responder

Referring now to Figure 3, this shows the action of the responder when it receives a connection request message.

(3-1) The action of the responder depends on whether any security information (LA3) is present in the connection request.

(3-2) If security information is present, the responder binds LA3 with R4, R5 and R6 to produce a resultant security level LA6. If LA6 has any empty ratings, the attempted connection has failed.

(3-3) If the attempted connection has not yet failed, it is now considered to have been successful. The responder returns a confirmation

message to the initiator, informing it that the connection has been successfully completed, and informing it of the final security level LA6 for the connection for those ratings in LA3. The responder then adopts this level LA6 as its view of the overall security level SLA for this connection.

(3-4) If, on the other hand, there is no security information in the connection request, the responder binds the available local security ratings R4, R5 and R6 to produce the security level LA6, and adopts this as its view of the overall security level SLA of the connection. As before, the responder returns a confirmation message to the initiator, but in this case, the message contains no security information.

Referring again to Figure 2, the action of the initiator on receiving a confirmation message is as follows.

(2-7) The initiator checks whether the confirmation message contains a security level with a subset of LA6's ratings.

(2-8) If so, the initiator adopts this subset of LA6 and the other ratings of LA3 as its view of the overall security level SLA of the connection.

(2-9) Otherwise, the initiator uses LA3 as its view of the overall security level.

In summary, it can be seen that where the initiator does not believe the responder to be capable of discussing security, it does not transmit any security information to it. In this case, both the initiator and responder rely solely on their own local knowledge of the security levels in the system to decide whether or not the connection succeeds, and each produces its own view of the overall security level for the connection.

On the other hand, where the initiator believes that the responder is capable of discussing security, a dialogue takes place between them to establish an agreed overall security level, based on the local views of both the initiator and the responder.

It should be noted that, in the described system, it is not necessary for the initiator and the responder to have a common security vocabulary; that is, one may consider security factors that the other is completely unaware of. This avoids the need to synchronise the security vocabulary of the servers, and avoids the need for unnecessary exchanges of security information which could, in itself, compromise security.

Claims

1. A distributed data processing system comprising a plurality of servers wherein each server separately maintains security information relating to security levels in the system, and wherein, in opera-

tion, when a first server initiates a connection with a second server, these two servers exchange security information to establish an overall security level for the connection based on a combination of the security information maintained by both servers.

5

2. A system according to Claim 1 wherein, in operation, if the security information maintained by the first server indicates that the second server cannot be trusted to receive security information, the servers exchange messages containing no security information and each server establishes its own security level for the connection based on its own locally held security information.

10

3. A system according to claim 1 or 2 wherein said security information comprises a set of security ratings for each server in the system.

15

4. A system according to claim 3 wherein each security rating comprises at least one security factor comprising at least one value.

5. A system according to claim 4, wherein the first server determines that the second server cannot be trusted to receive security information if the security rating of the second server, as viewed by the first server, contains only security factors with only one value.

20

25

30

35

40

45

50

55

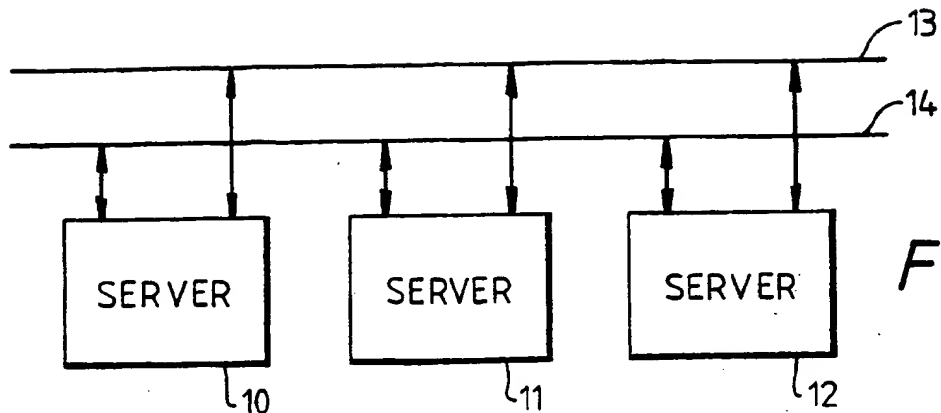


Fig. 1.

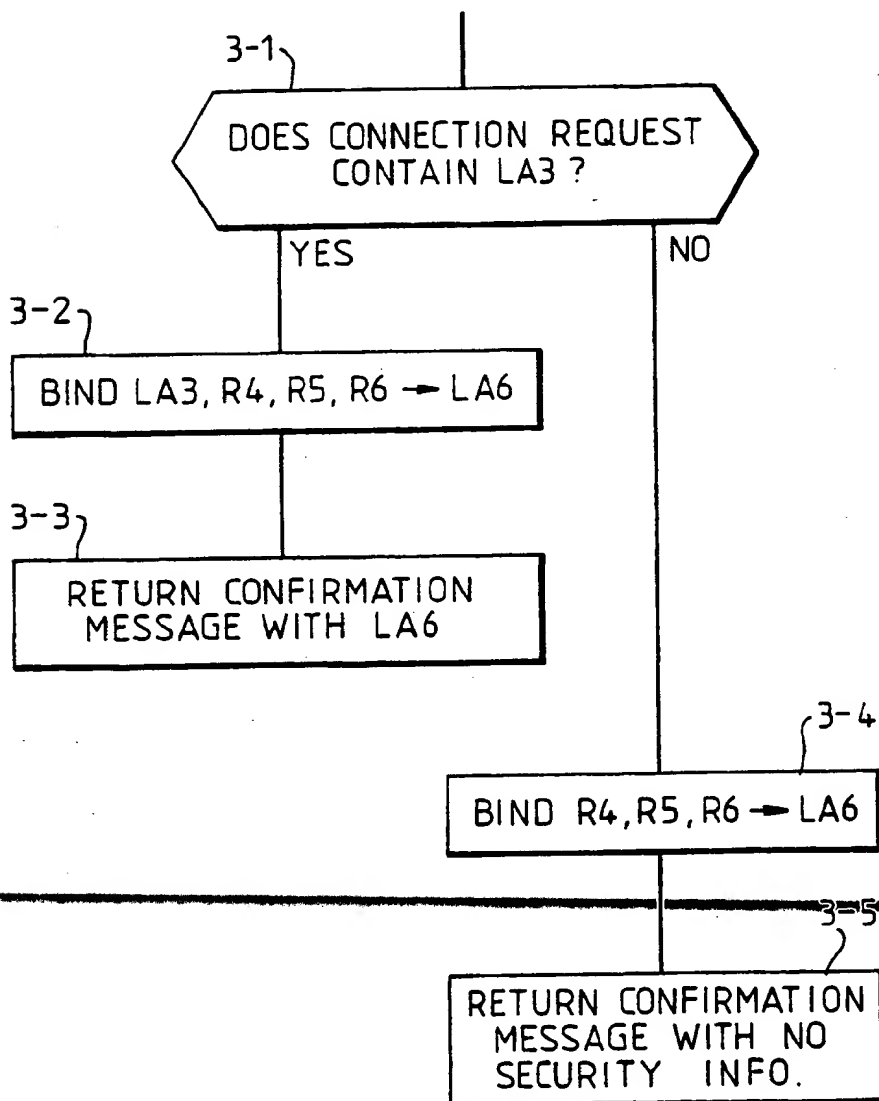
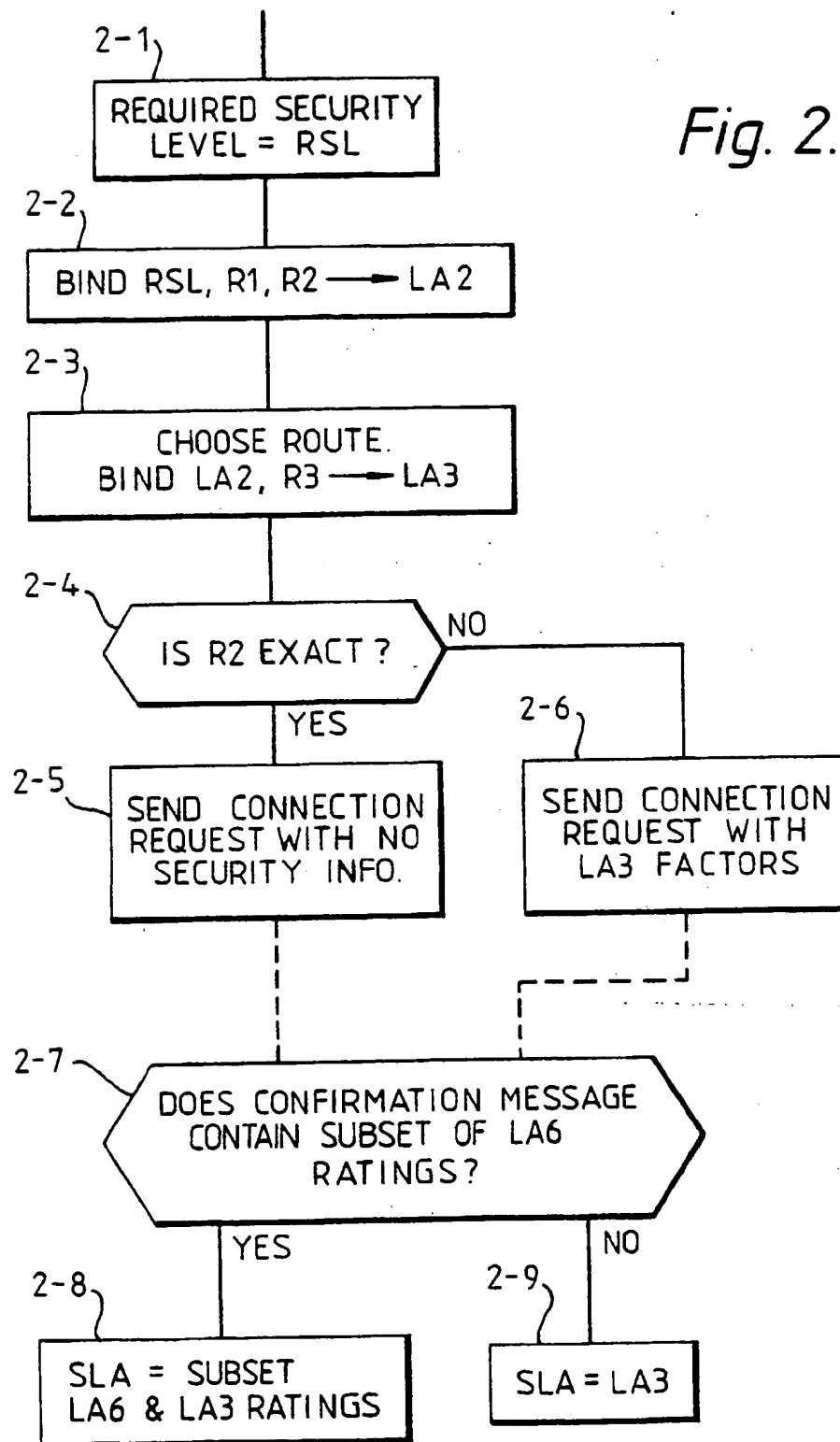


Fig. 3.

Fig. 2.



THIS PAGE BLANK (USPTO)

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) Publication number:

0 409 397 A3

(12)

EUROPEAN PATENT APPLICATION(21) Application number: **90306141.4**(51) Int. Cl.⁵: **G06F 1/00, G06F 9/46**(22) Date of filing: **06.06.90**(30) Priority: **20.07.89 GB 8916586**(43) Date of publication of application:
23.01.91 Bulletin 91/04(84) Designated Contracting States:
BE DE FR GB IT(88) Date of deferred publication of the search report:
22.04.92 Bulletin 92/17(71) Applicant: **INTERNATIONAL COMPUTERS
LIMITED**

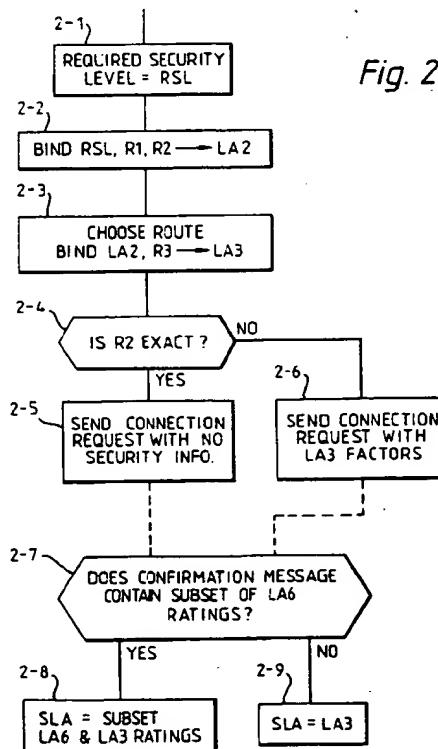
**ICL House
Putney, London, SW15 1SW(GB)**

(72) Inventor: **McVitie, David Glen
Brunswick House, Brunswick Street
Congleton, Cheshire CW12 1QF(GB)**

(74) Representative: **Guyatt, Derek Charles Patents
and Licensing International Computers
Limited et al
Six Hills House London Road
Stevenage, Herts, SG1 1YB(GB)**

(54) **Distributed data processing system.**

(57) A security mechanism is described for a distributed data processing system. Each server in the system maintains a set of security ratings giving its view of the security levels within the system. When a first server wishes to initiate a connection with a second server, the two servers exchange security information, by means of messages, so as to establish an overall security level for the connection, based on a combination of the security information maintained by both servers. However, if the first server decides that the second server cannot be trusted to discuss security, messages are exchanged containing no security information, and each server establishes its own security level for the connection, based on its own locally held security information.

**EP 0 409 397 A3**



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number

EP 90 30 6141

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
X	COMPCON 89, IEEE, FEB. 27-MARCH 3, 1989 SAN FRANCISCO, CA, PAGES 338-341 R.M. WONG ET AL.: "ISSUES IN SECURE DISTRIBUTED OPERATING SYSTEM DESIGN"	1-3	G06F1/00 G06F9/46
A	* page 340, left column, paragraph 5.1 *	4	
A	PROCEEDINGS, IEEE, SECURITY AND PRIVACY, MAY 1-3, 1989, OAKLAND, CA PAGES 56-63 LI GONG: "A SECURE IDENTITY-BASED CAPABILITY SYSTEM" * page 57, right column, line 40 - page 59, right column, line 9 *	1, 3, 4	
			TECHNICAL FIELDS SEARCHED (Int. Cl.5)
			G06F
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 25 FEBRUARY 1992	Examiner WEISS P.
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 (01.92) (P0001)

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

THIS PAGE BLANK (USPTO)

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

- (i) the claim is unchanged;
- (ii) the claim is cancelled;
- (iii) the claim is new;
- (iv) the claim replaces one or more claims as filed;
- (v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the same time of filing the amendments with the International Bureau, also file a copy of such amendments with the International Preliminary Examining Authority (see Rule 62.2(a), first sentence).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, where upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.

THIS PAGE BLANK (USPTO)
